

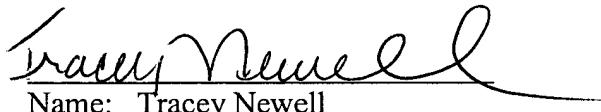


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Andrew Ginter, et al. :
Serial No.: 10/815,222 : Examiner: Not Yet Assigned
Filed: March 31, 2004 : Art Unit: Not Yet Assigned
For: EVENT MONITORING AND : Atty. Docket: VRS-00101
MANAGEMENT :
:

Certificate of Mailing

I hereby certify that the foregoing document is being deposited with the United States Postal Service, postage prepaid, first class mail, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 20th day of August, 2004.



Name: Tracey Newell

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith on Form PTO-1449 is a listing of documents known to Applicant and/or their attorney in compliance with the requirements of 37 C.F.R. § 1.56. Copies of the documents are also being submitted.

In accordance with 37 C.F.R. 1.97(b)(4), Applicant believes that no fee is due since this Information Disclosure Statement (IDS) is submitted before the mailing of the first Office Action.

The Examiner is respectfully requested to initial the space adjacent to each document on the PTO-1449 form and return a copy of the PTO-1449 form to confirm that these documents have been considered by the Examiner and made of record in this application.

Although we believe that we have appropriately provided for any fees due in connection with this submission, the Commissioner is authorized to credit any overpayment or charge any deficiencies to/from our **Deposit Account No. 03-1721**. Two originally-executed copies of this form are being submitted.

Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at (617) 248-4042.

Respectfully submitted,
CHOATE, HALL & STEWART



Anne E. Saturnelli, Reg. No. 41,290

Patent Group
CHOATE, HALL & STEWART
Exchange Place
53 State Street
Boston, MA 02109
Tel: (617) 248-5000
Fax: (617) 248-4000

Date: August 20, 2004

Customer Number 26339



Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	10/815,222
				Filing Date	March 31, 2004
				First Named Inventor	Andrew Ginter, et al.
				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	1	of	6	Attorney Docket Number	VRS-00101

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (<i>if known</i>)			
		US-6,219,719 B1	Apr. 17, 2001	Lars Oliver Graf	
		US-6,212,581 B1	Apr. 3, 2001	Lars O. Graf	
		US-5,619,656	Apr. 8, 1997	Lars O. Graf	
		US-			

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appeal
		Country Code ³ - Number ⁴ - Kind Code ⁵ (<i>if known</i>)			
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>

Examiner Signature		Date Considered
--------------------	--	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3.) ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

3727357v1

Did not receive C and K of Non-patent Documents

Substitute for form 1449B/PTO					<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT					Application Number	10/815,222
(Use as many sheets as necessary)					Filing Date	March 31, 2004
					First Named Inventor	Andrew Ginter, et al.
					Art Unit	Not Yet Assigned
					Examiner Name	Not Yet Assigned
Sheet	2	of	6		Attorney Docket Number	VRS-00101

NON-PATENT LITERATURE DOCUMENTS						
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.				T ²
	A	SnortUsers Manual, Copyright ©1998-2003 MARTIN ROESCH, Copyright ©2001-2003 CHRIS GREEN, Copyright © 2003 Sourcefire, Inc. – http://www.snort.org/docs/snort_manual				<input type="checkbox"/>
	B	Arpwatch.txt, 4 th Berkeley Distribution, October 8, 2000, Arpwatch(8), ftp://ftp.ee.lbl.gov/arpwatch.tar.gz				<input type="checkbox"/>
	C	RTAP FOR UNIX® Integrator's Guide, August 2000, Copyright ©1998-2000 Hewlett-Packard (Canada) Ltd.				<input type="checkbox"/>
	D	Linux Journal - Issue 117: Monitoring Hard Disks with SMART, posted on January 1, 2004 by BRUCE ALLEN, www.linuxjournal.com/article.php?sid=6983				<input type="checkbox"/>
	E	Smartmontools Home Page, maintained by BRUCE ALLEN, Copyright ©2002-2004, http://smartmontools.sourceforge.net/				<input type="checkbox"/>
	F	RFC 1700: Assigned Numbers by J. REYNOLDS and J. POSTEL, October 1994, ISI, www.cse.ohio-state.edu/cgi-bin/rfc/rfc1700.html				<input type="checkbox"/>
	G	RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware Abstract by DAVID C. PLUMMER, November 1982, www.cse.ohio-state.edu/cgi-bin/rfc/rfc0826.html http://smartmontools.sourceforge.net/				<input type="checkbox"/>
	H	SMARTD.CONF – SMART Disk Monitoring Daemon Configuration File (online help describing the SMART monitoring tools project), http://smartmontools.sourceforge.net/man/smartd.conf.5.html				<input type="checkbox"/>
	I	SMARTD – SMART Disk Monitoring Daemon (online help describing the SMART monitoring tools project), http://smartmontools.sourceforge.net/man/smartd.8.html				<input type="checkbox"/>
	J	SMARTCTL – Control and Monitor Utility for SMART Disks (online help describing the SMART monitoring tools project), http://smartmontools.sourceforge.net/man/smartctl.8.html				<input type="checkbox"/>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

<p>Substitute for form 1449B/PTO</p> <p>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</p> <p>(Use as many sheets as necessary)</p>				Complete if Known	
				Application Number	10/815,222
				Filing Date	March 31, 2004
				First Named Inventor	Andrew Ginter, et al.
				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	3	of	6	Attorney Docket Number	VRS-00101

NON-PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²	
	K	Snort 2.0 Intrusion Detection, 2003, by JAY BEALE, JAMES C. FOSTER, JEFFREY POSLUNS and BRIAN CASWELL, Syngress Publishing, Inc., Rockland, MA, ISBN: 1-931836-74-4	<input type="checkbox"/>	
	L	Hardware Monitoring by lm_sensors, Copyright © 1999-2004 The Lm_sensors Group, http://secure.netroedge.com/~lm78	<input type="checkbox"/>	
	M	Sensors FAQ for lm_sensors version 2.12, Copyright © 1998-2004, FRODO LOOJAARD, PHILIP EDELBROCK and MARK STUDEBAKER, http://www2.lm-sensors.nu/~lm78/cvs/lm_sensors2/doc/lm_sensors-FAQ.html .	<input type="checkbox"/>	
	N	Tripwire.org, http://www.tripwire.org/ Tripwire Open Source, Linux Edition FAQ, http://www.tripwire.org/qanda/index.php Downloads, http://www.tripwire.org/downloads/index.php	<input type="checkbox"/>	
	O	The Design and Implementation of Tripwire: A File System Integrity Checker by GENE H. KIM and EUGENE H. SPAFFORD, © 1994 ACM	<input type="checkbox"/>	
	P	fverify(8), http://h30097.www3.hp.com/docs/base_doc/DOCUMENTATION/V51_HTML/MAN/INDEXES/INDEX_F.HTM	<input type="checkbox"/>	
	Q1	RTAP - Increasing Visibility and Return on Real-time Information with a Mission Critical Supervisory Platform by Verano, Inc. © Copyright 2003, http://www.verano.com/general_downloads/rtap_overview.pdf	<input type="checkbox"/>	
	Q2	RTAP™ Technical Overview, http://www.verano.com/general_downloads/RTAP_TechDataSheet_July04.pdf	<input type="checkbox"/>	
	R	Open – Proven network and security threat management – Products http://www.open.com/products/systemwatch/sys_architecture.shtml http://www.open.com/products/systemwatch/sys_arch_console.shtml http://www.open.com/products/systemwatch/sys_arch_agent.shtml © 2000 – 2004 OpenService, Inc.	<input type="checkbox"/>	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute for form 1449B/PTO					<i>Complete if Known</i>	
					Application Number	10/815,222
					Filing Date	March 31, 2004
					First Named Inventor	Andrew Ginter, et al.
					Art Unit	Not Yet Assigned
					Examiner Name	Not Yet Assigned
Sheet	4	of	6	Attorney Docket Number	VRS-00101	

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	S	Open - Proven network and security threat management – Enterprise Security Information Management, Event Correlation and Log Analysis, http://www.open.com/index_core.htm	<input type="checkbox"/>
	T	Open - Proven network and security threat management – Solutions, http://www.open.com/solutions/solutions.shtml	<input type="checkbox"/>
	U	Open - Proven network and security threat management – What is Event Correlation, http://www.open.com/solutions/correlation.shtml	<input type="checkbox"/>
	V	Open - Proven network and security threat management – Correlation Semantics – What's in a Name, http://www.open.com/solutions/SimSemantics.shtml	<input type="checkbox"/>
	W	Open - Proven network and security threat management – Overcoming the Barriers to Successful Security Event Management, http://www.open.com/solutions/successful_SEM.shtml	<input type="checkbox"/>
	X	Open - Proven network and security threat management – What's Magic About Security Event Correlation, http://www.open.com/solutions/magicquadrant.shtml	<input type="checkbox"/>
	Y	Open - Proven network and security threat management – Case Study: Countrywide Home Loans, http://www.open.com/solutions/countrywide.shtml	<input type="checkbox"/>
	Z	Open - Proven network and security threat management – Case Study: Stadtwerke Dusseldorf AG, http://www.open.com/solutions/stadtwerke.shtml	<input type="checkbox"/>
	AA	Open - Proven network and security threat management – Products – Enterprise Security Information Management and Threat Correlation, http://www.open.com/products/products.shtml	<input type="checkbox"/>
	AB	Open - Proven network and security threat management – Partners – Introducing Security Threat Manager/Surveyor™, http://www.open.com/partners/partners_surveyor.shtml	<input type="checkbox"/>
	AC	Open - Proven network and security threat management – Security Threat Manager™ v2.0, http://www.open.com/products/threatmanager/STM2_FullLog.shtml	<input type="checkbox"/>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

Substitute for form 1449B/PTO				Complete if Known	
				Application Number	10/815,222
				Filing Date	March 31, 2004
				First Named Inventor	Andrew Ginter, et al.
				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	5	of	6	Attorney Docket Number	VRS-00101

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	AD	Open - Proven network and security threat management – Products – Open NerveCenter Overview, http://www.open.com/products/nervecenter/nervecenter.shtml	<input type="checkbox"/>
	AE	Open - Proven network and security threat management – News – OpenService Appoints Michael Ruffolo to Board of Directors, http://www.open.com/news/040719.shtml	<input type="checkbox"/>
	AF	Open - Proven network and security threat management – News – Press Releases, http://www.open.com/news/releases.shtml	<input type="checkbox"/>
	AG	Open - Proven network and security threat management – News – Press Coverage Archive, http://www.open.com/news/coverage.shtml	<input type="checkbox"/>
	AH	Open - Proven network and security threat management – News – Seminars, http://www.open.com/news/events.shtml	<input type="checkbox"/>
	AI	Open - Proven network and security threat management – News – Newsletter Information, http://www.open.com/news/newsletters.shtml	<input type="checkbox"/>
	AJ	Open – Security Threat Manager™ At Work	<input type="checkbox"/>
	AK	Open – Network Security Management – Active Event Monitoring and Management of Your Security Infrastructure, © 2002 OpenService, Inc.	<input type="checkbox"/>
	AL	SELinux Documentation, http://www.nsa.gov/selinux/info/docs.cfm	<input type="checkbox"/>
	AM	Integrating Flexible Support for Security Policies into the Linux Operating System by PETER LOSCOCCO and STEPHEN SMALLEY, FREENIX Track: 2001 USENIX Annual Technical Conference June 2001	<input type="checkbox"/>
	AN	Meeting Critical Security Objectives with Security-Enhanced Linux by PETER A. LOSCOCCO and STEPHEN D. SMALLEY, 2001 Ottawa Linux Symposium	<input type="checkbox"/>
	AO	Securing the X Window System with SELinux by DOUG KILPATRICK, WAYNE SALAMON and CHRIS VANCE, initial version: January 2003, revised version: March 2003	<input type="checkbox"/>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

Substitute for form 1449B/PTO				<i>Complete if Known</i>	
				Application Number	10/815,222
				Filing Date	March 31, 2004
				First Named Inventor	Andrew Ginter, et al.
				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	6	of	6	Attorney Docket Number	VRS-00101

NON-PATENT LITERATURE DOCUMENTS					
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			T ²
	AP	Configuring the SELinux Policy by STEPHEN SMALLEY, initial version: February 2002, revised version: January 2003			<input type="checkbox"/>
	AQ	Implementing SELinux as a Linux Security Module by STEPHEN SMALLEY, CHRIS VANCE and WAYNE SALAMON, initial version: December 2001, revised version: May 2002			<input type="checkbox"/>
	AR	Integrating Flexible Support for Security Policies into the Linux Operating System by PETER LOSCOCCO and STEPHEN SMALLEY, first published: December 2000, last revised: February 2001			<input type="checkbox"/>
	AS	A Security Policy Configuration for the Security-Enhanced Linux by STEPHEN SMALLEY and TIMOTHY FRASER, first published: December 2000, last revised: February 2001			<input type="checkbox"/>
	AT	2003 Ottawa Linux Symposium BOF Presentation by STEPHEN D. SMALLEY, 2003 Ottawa Linux Symposium SELinux "Birds of a Feather" Session			<input type="checkbox"/>
	AU	Security-Enhanced Linux 2001 Kernel Summit Presentation by PETER A. LOSCOCCO, 2001 Linux 2.5 Kernel Summit			<input type="checkbox"/>
	AV	Press Releases: OpenService Announces Security Threat Manager Version 2, http://www.open.com/news/releases.jsp?file=031210.jsp			<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2